МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра вычислительной техники и защиты информации

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

УЧЕБНОЙ ДИСЦИПЛИНЫ

«ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ»

Уровень подготовки: высшее образование – магистратура

Направление подготовки магистров
10.04.01 Информационная безопасность
(код и наименование направления подготовки)

Направленность подготовки
Информационная безопасность
(наименование программы подготовки)

Квалификация (степень) выпускника
Магистр

Форма обучения
очная

Разработана в соответствии

с ФГОС ВПО, Приказ МОиН РФ от 28.10.2009, № 497

Актуализирована в соответствии

с ФГОС ВО, Приказ МОиН РФ от 01.12.2016, № 1513

Уфа 2016

Исполнитель:

доцент каф. ВТиЗИ		В.Е.Кладов
должность	*личная подпись*	*расшифровка подписи*

Заведующий кафедрой

ВТиЗИ		В.И.Васильев
наименование кафедры	*личная подпись*	*расшифровка подписи*

1. Место дисциплины в структуре образовательной программы

Дисциплина «Защищенные информационно-вычислительные системы» является дисциплиной базовой части ОПОП по направлению подготовки 10.04.01 Информационная безопасность, направленность: «Информационная безопасность».

Рабочая программа составлена в соответствии с требованиями:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 090900 Информационная безопасность (квалификация "магистр"), утвержденного приказом Министерства образования и науки Российской Федерации от 28 октября 2009 г. № 497;

Рабочая программа актуализирована в соответствии с требованиями:

- Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 10.04.01 Информационная безопасность (квалификация "магистр"), утвержденного приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. № 1513.

Является неотъемлемой частью основной образовательной профессиональной программы (ОПОП).

Целью освоения дисциплины является формирование у будущих магистров в области информационной безопасности теоретических знаний и практических навыков для решения научно-исследовательских и прикладных задач связанных с проектированием и построением защищенных информационно-вычислительных систем.

Задачи:

- научить проектировать сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты;
- развить способность анализировать угрозы информационной безопасности объектов и разрабатывать методы противодействия им;
- познакомить с архитектурой и принципами функционирования DLP систем;
- привить навыками поиска и анализа инцидентов информационной безопасности;
- научить методам борьбы с внутренними нарушителями (инсайдерами);
- привить способность самостоятельно осваивать и адаптировать к защищаемым объектам современные методы обеспечения информационной безопасности;
- научить навыкам администрирования DLP, SIEM систем, средств управления и мониторинга корпоративными вычислительными сетями;
- изучить методы защиты веб-серверов и веб-приложений и привить практические навыки в этом;
- научить моделировать возможные способы удаленных атак на компьютерные системы и применять современные методы противодействия им.

Дисциплина является самостоятельным элементом в системе подготовки научно-педагогических кадров высшей квалификации. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- теоретические основы компьютерной безопасности;
- управление информационной безопасностью.

В дисциплине «Защищенные информационно-вычислительные системы» определяются теоретические основы и практические навыки, при освоении которых обучающийся способен приступить к прохождению практик и выполнять научные исследования в соответствующей предметной области.

Входные компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции*	Название дисциплины (модуля), практики, научных исследований, сформировавших данную компетенцию
1	способностью анализировать направления развития (телеком-муникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	ПК-1	Базовый уровень	Управление информационной безопасностью
2	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	ПК-7	Базовый уровень	Теоретические основы компьютерной безопасности
3	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	ПК-5	Базовый уровень	Теоретические основы компьютерной безопасности
4	способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	ПК-14	Базовый уровень	Управление информационной безопасностью

*- ***пороговый уровень*** *дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;*

-базовый уровень *позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;*

-повышенный уровень *предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.*

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), практики, научных исследований для которых данная компетенция является входной
1	способность разрабатывать, системы, комплексы, средства и технологии обеспечения информационной безопасности	ПК-2	Повышенный уровень	Производственная практика Преддипломная практика Подготовка магистерской диссертации
2	способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	ПК-3	Повышенный уровень	Производственная практика Преддипломная практика Подготовка магистерской диссертации
3	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	ПК-7	Повышенный уровень	Производственная практика Преддипломная практика Подготовка магистерской диссертации

2. Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций.

Планируемые результаты обучения по дисциплине

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1	способность разрабатывать, системы, комплексы, средства и технологии обеспечения информационной безопасности	ПК-2	Архитектуру и принципы функционирования DLP систем, средств управления мониторинга и управления мониторинга корпоративной IT средой	Осуществлять выбор функциональной структуры обеспечения информационной безопасности	Навыками поиска и анализа инцидентов информационной безопасности
2	способность проводить обоснование состава, характеристик и функциональных	ПК-3	Возможные способы реализации удаленных атак на компьютерные системы и методы	Моделировать возможные способы удаленных атак на компьютерные системы и применять	Навыками администрирования средств управления и мониторинга корпоративны-

	возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов		противодействия им; Основные методы защиты информационных процессов в веб-серверах и веб-приложениях	современные методы противодействия им Уметь самостоятельно осваивать и адаптировать к защищаемым объектам современные методы обеспечения информационной безопасности	ми вычислительными сетями, Навыками защиты веб-серверов и веб-приложений
3	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	ПК-7	Принципы построения и работы систем анализа и мониторинга систем	-	- навыками практического анализа угроз информационной безопасности , применяя для этого SIEM системы, сканеры уязвимостей, средства управления и мониторинга корпоративной IT средой

3. Содержание и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).

Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.	Трудоемкость, час.
	1 семестр	2 семестр
Лекции (Л)	–	12
Практические занятия (ПЗ)	–	18
Лабораторные работы (ЛР)	–	8
КСР	–	4
Курсовая проект работа (КР)	–	
Расчетно - графическая работа (РГР)	–	
Самостоятельная работа (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам, рубежному контролю и т.д.)	–	93
Подготовка и сдача экзамена	–	
Подготовка и сдача зачета (контроль)	–	9
Вид итогового контроля (зачет, экзамен)	–	зачет

Содержание разделов и формы текущего контроля

№	Наименование и содержание раздела	Количество часов						Литература, рекомендуемая студентам*	Виды интерактивных образовательных технологий**
		Аудиторная работа				СРС	Всего		
		Л	ПЗ	ЛР	КСР				
1	**DLP системы.** Понятие DLP систем. Назначение и принципы функционирования, решаемые задачи. Архитектура, принципы построения и организации работы. Методы контроля пользователей. Технические возможности получения информации об активности работников. Виды перехвата информации. Состав и взаимосвязь DLP систем. Особенности реализации сетевого перехвата траффика. Реализация перехвата почтовых сообщений путем интеграции с почтовыми серверами. Особенности реализации агентского перехвата траффика. Поиск по перехваченным документам. Поиск по словарю. Поиск «похожих». Поиск по атрибутам документов. поиск нераспознанных документов. Запросы с использованием регулярных выражений. Фразовый поиск. сложные запросы с комбинированием нескольких простых запросов. Запросы с использованием цифровых отпечатков. Автоматический мониторинг информационных потоков. Формирование отчетов об активности пользователей и инцидентах.	4	4	4	1	24	37	Р 6.1, №1 Р 6.2, №5 Р 6.2, №2 Р 6.2, №4	*лекция-визуализация, проблемное обучение, обучение на основе опыта, компьютерная симуляция*
2	**SIEM системы.** Понятие SIEM (Security Information and Event Management) систем**.** Системы анализа и мониторинга событий. Спектр применения. Задачи и возможности SIEM систем. Архитектура и источники SIEM систем. Наиболее популярные SIEM системы: IBM QRadar, HP ArcSign, MaxPatrol SIEM. SIEM решения фирмы SearchInform.	2	4		1	12	19	Р 6.1, №1 Р 6.2, №3	*лекция-визуализация, проблемное обучение, обучение на основе опыта*

3	**Средства управления и мониторинга корпоративной IT средой.** Microsoft System Center- комплексное решение по изменению и управлению конфигурациями для платформ Microsoft. Configuration Manager. Средство мониторинга инфраструктур Operations Manager. Средство интеграции и автоматизации IT процессов System Center Orchestrator. Решение для управления виртуальным центром обработки данных Virtual Machine Manager (VMM). Решение для резервного копирования и восстановления рабочих нагрузок Microsoft Data Protection Manager (DPM). Единая консоль управления общедоступными и частными облаками System Center App Controller	4		4	1	27	36	Р 6.1, №1 Р 6.2, №5 Р 6.2, №1	*лекция-визуализация, проблемное обучение, обучение на основе опыта, компьютерная симуляция*
4	**Защита веб-серверов и веб приложений.** Особенности веб-сервера IIS. Файлы конфигурации IIS, Авторизация пользователей. Учетные записи IIS, Аутентификация. Основные методы. Правила авторизации. Протокол SSL. Сопоставление сертификатов пользователей в IIS. Разграничение доступа. Аудит IIS. Особенности веб-сервера Apache. Структура каталогов, система конфигурации. Аутентификация и авторизация. Разграничение доступа к ресурсам веб-сервера. Журналы. Классификация удаленных атак на распределенные вычислительные системы. Средства защиты веб-приложений. Выделение Web Application Firewall в отдельный класс устройств. Принцип работы WAF, Тенденции развития WAF. Imperva. Aplication Firewall фирмы Positive Technologies.	4	10		1	30+3 (контроль)	48	Р 6.1, №1 Р 6.2, №5 Р 6.2, №3 Р 6.2, №4	*лекция-визуализация, проблемное обучение, обучение на основе опыта, компьютерная симуляция*

Занятия, проводимые в интерактивной форме, составляют 9,5% от общего количества аудиторных часов по дисциплине.

Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1,2	1	DLP системы Infowatch Traffic Monitor	4
3, 4	2	SIEM система Qradar	4
5	4	Защита информации в веб-сервере IIS	2
6	4	Защита информации в веб-сервере Apache	2
7	4	Возможные пути реализации злоумышленниками удаленных атак	2
8,9	4	WAF	4

Лабораторные работы

№ занятия	№ раздела	Тема	Кол-во часов
1	1	DLP системы Falcongaze Secure Tower	4
2	3	Microsoft System Center	4

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1 Основная литература

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : [учебное пособие] / В. Ф. Шаньгин .— Москва : Форум : Инфра-М, 2013.— 415, [1] с. : ил. ; 21 см .— (Профессиональное образование)

1.2 Дополнительная литература

1.Основы информационной безопасности [Электронный ресурс] : [учеб. пособие для студ., обуч по спец. в области информационной безопасности] / Е. Б. Белов [и др.] .— Москва : Горячая линия-Телеком, 2011 .— 544 с. : ил. — Библиогр. в конце гл. — Доступ по логину и паролю из сети УГАТУ .— ISBN 5-93517-292-5 .— <URL:http://e.lanbook.com/view/book/5121/page2/>.

2.Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : [учебное пособие для студентов высших учебных заведений, обучающихся по направлению «Информатика и вычислительная техника»] / В. Ф. Шаньгин .— Москва : ДМК ПРЕСС, 2012 .— 592 с. — Доступ по логину и паролю из сети УГАТУ .— ISBN 978-5-94074-637-9 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=3032>.

3.Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] : [учебное пособие для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника»] / В. Ф. Шаньгин .— Москва : ДМК ПРЕСС, 2010 .— 544 с. — Доступ по логину и паролю из сети УГАТУ .— ISBN 978-5-94074-518-1 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122>.

4. Гришина, Н. В. Комплексная система защиты информации на предприятии : [учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информации"] / Н. В. Гришина .— Москва : ФОРУМ, 2014.— 238 с. : ил. ; 22 см .— (Профессиональное образование)

5. Сердюк, В. А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В. А. Сердюк ; Государственный университет, Высшая школа экономики .— Москва : Издательский дом Государственного университета- Высшей школы экономики, 2011 .— 572 с. ; 21 см .— ISBN 978-5-7598-0698-1

6.3. Интернет-ресурсы (электронные учебно-методические издания, лицензионное программное обеспечение)

На сайте библиотеки http://library.ugatu.ac.ru/ в разделе «Информационные ресурсы», подраздел «Доступ к БД» размещены ссылки на интернет-ресурсы.

Обучающимся обеспечен доступом к электронным ресурсам и информационным справочным системам, перечисленным в таблице

Таблица

№	Наименование ресурса	Объем фонда электронных ресурсов	Доступ	Реквизиты договоров с правообладателями
1.	ЭБС «Лань» http://e.lanbook.com/	41716	С любого компьютера, имеющего выход в Интернет, после регистрации в ЭБС по сети УГАТУ	Договор № ЕД – 1185/0208-16 от 08.08.2016
2.	ЭБС Ассоциации «Электронное образование Республики Башкортостан» http://e-library.ufa-rb.ru	1225	С любого компьютера, имеющего выход в Интернет, после регистрации в АБИС «Руслан» на площадке библиотеки УГАТУ	Учредительный договор Ассоциации образовательных организаций «Электронное образование Республики Башкортостан» от 29.11.2013
3.	Консорциум аэрокосмических вузов России http://elsau.ru/	1235	С любого компьютера, имеющего выход в Интернет, после регистрации в АБИС «Руслан» на площадке библиотеки УГАТУ	Договор о сетевом взаимодействии от 15.12.2014
4.	Электронная коллекция образовательных ресурсов УГАТУhttp://www.library.ugatu.ac.ru/cgi-bin/zgate.exe?Init+ugatu-fulltxt.xml,simple-fulltxt.xsl+rus	528	С любого компьютера по сети УГАТУ	Свидетельство о регистрац. №2012620618 от 22.06.2012
5.	Электронная библиотека диссертаций РГБ http://dvs.rsl.ru	885 898 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор №2255/0208-15 от 23.12.2015
6.	База данных Proquest Dissertations and Theses Global http://search.proquest.com/	более 3,5 млн. диссертаций и	С любого компьютера по сети УГАТУ, имеющего выход в	В рамках Государственного контракта от 17.02.2016 г.

		дипломных работ	Интернет	№14.596.11.0014 между Министерством образования и науки РФ и Государственной публичной научно-технической библиотекой России (далее ГПНТБ России) Сублиц. договор №ProQuest/15152/0208-16 от 02.06.2016
7.	СПС «КонсультантПлюс»	2007691 экз.	По сети УГАТУ	Договор 3К-2318/0106-15 от 30.12.2015
8.	СПС «Гарант»	6139026 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор 15\0208-16 от 15.03.2016
9.	ИПС «Технорма/Документ»	36939 экз.	Локальная установка: библиотека УГАТУ-5 мест; кафедра стандартизации и метрологии-1место; кафедра начертательной геометрии и черчения-1 место	Договор № АОСС/914-15 № 989/0208-15 от 08.06.2015.
10.	Научная электронная библиотека eLIBRARY* http://elibrary.ru/	9919 полнотекстовых журналов	С любого компьютера, имеющего выход в Интернет, после регистрации в НЭБ на площадке библиотеки УГАТУ	ООО «НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА». № 07-06/06 от 18.05.2006
11.	Патентная база данных компании Questel Orbit* http://www.orbit.com	55 млн. документов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России

				Сублиц. договор№Questel/15146/0208-16 от 02.06.2016
12.	Научные полнотекстовые журналы издательства Taylor& Francis Group* http://www.tandfonline.com/	1700 наимен. журнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №T&F/15144/0208-16 от 02.06.2016
13.	Научные полнотекстовые журналы издательства Sage Publications* http://online.sagepub.com/	790 наимен. жрнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Sage/15147/0208-16 от 02.06.2016
14.	Научные полнотекстовые журналы издательства Oxford University Press* http://www.oxfordjournals.org/	255 наимен. Журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №OUP-15143/0208-16 от 02.06.2016
15.	База данных Computers & Applied Sciences Complete компании EBSCO Publishing http://search.ebscohost.com	1000 наим. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством

				образования и науки РФ и ГПНТБ России Сублиц. договор №CASC/151 50/0208-16 от 02.06.2016
16.	Научный полнотекстовый журнал Science The American Association for the Advancement of Science http://www.sciencemag.org	1 наимен. журнала.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Science/151 45/0208-16 от 02.06.2016
17.	Научные полнотекстовые журналы Американского института физики http://scitation.aip.org/	18 наимен. журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №AIP/151 48/0208-16 от 02.06.2016
18.	Научные полнотекстовые ресурсы Optical Society of America* http://www.opticsinfobase.org/	19 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №OSA/151 49/0208-16 от 02.06.2016
19.	База данных GreenFile компании EBSCO* http://www.greeninfoonline.com	5800 библиографич записей, частично с полными	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ предоставлен компанией EBSCO российским организациям-

		текстами		участникам консорциума НЭИКОН (в т.ч. УГАТУ - без подписания лицензионного договора)
20.	Реферативная база данных INSPEC компании EBSCO Publishing http://search.ebscohost.com	Более 11 млн. библиографич записей		В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. Договор №INSPEC/151 51/0208-16 от 02.06.2016
21.	Архив научных полнотекстовых журналов зарубежных издательств*- http://archive.neicon.ru Annual Reviews (1936-2006) Cambridge University Press (1796-2011) цифровой архив журнала Nature (1869- 2011) Oxford University Press (1849– 1995) SAGE Publications (1800-1998) цифровой архив журнала Science (1880 -1996) Taylor & Francis (1798-1997) Институт физики Великобритании The Institute of Physics (1874-2000)	2361 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ предоставлен российским организациям-участникам консорциума НЭИКОН (в т. ч. УГАТУ - без подписания лицензионного договора)

* Периодические издания получены по Гранту и на баланс библиотеки не принимались.

7 Образовательные технологии

Для достижения наиболее эффективных результатов освоения дисциплины при реализации различных видов учебной работы применяются информационные технологии (использование компьютерных тестирующих средств оценки уровня знаний обучаемых, использование мультимедийного сопровождения лекций, электронных мультимедийных учебных пособий и др.) и интерактивные методы и технологии обучения (проблемные лекции, лекции-визуализации, технология проблемного обучения, технология развития критического мышления, групповая работа), с учетом содержания дисциплины и видов занятий, предусмотренных учебным планом.

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
2	Л	Лекция-визуализация	2
	ПР	Кейс задачи	2
Итого:			4

Формы работы студентов: лекционные занятия, лабораторные работы, практические занятия, решение кейс-задач, выступление с докладами, решение тестов, ответы на контрольные вопросы.

Дисциплина разбита на модули, представляющие собой логически завершенные части курса и являющиеся теми комплексами знаний и умений, которые подлежат контролю.

Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала.

В качестве организованной самостоятельной работы студента рекомендуется выступление с докладами по выбранной заранее тематике. При подготовке доклада студент должен в соответствии с требованиями к оформлению сформулировать проблему, актуальность, поставить цель и задачи исследования, сделать самостоятельный вывод о состоянии и путях решения заданной проблемы.

Для успешной подготовки к итоговому контролю необходимо выполнить следующие контрольные мероприятия:

1. Выполнить лабораторные работы по всем темам дисциплины. Выполнение лабораторных работ требует заполнения отчетов, которые составляются в электронном виде. Файлы отчета с материалами выполненных заданий лабораторных работ должны быть представлены преподавателю. В отчетах должна быть представлена следующая информация: тема работы; цель работы; общая постановка задачи; индивидуальные данные для выполнения работы (№ варианта); результаты выполнения работы; ответы на контрольные вопросы.

2. Выполнены все кейс-задачи. Решение кейс-задач требует представления отчетов, которые составляются в электронном виде. Файлы отчета с материалами выполненных заданий должны быть представлены преподавателю. В отчетах должна быть представлена следующая информация: тема работы; цель работы; общая постановка задачи; индивидуальные данные для выполнения задачи (№ варианта); результаты выполнения каждого пункта задачи; ответы на контрольные вопросы и тесты.

3. Пройти промежуточное тестирование по окончанию освоения очередного модуля учебной дисциплины.

Если не сдана хотя бы одна лабораторная работа или не пройден хотя бы один тест студент не допускается к зачету.

В случае если защищены все лабораторные работы, успешно выполнены все кейс-задачи и пройдены все тесты по разделам, и общий балл составляет 61 и выше студенту зачет по дисциплине проставляется автоматом. Для студентов, набравших менее 61 балла зачет проводится в аудитории по вопросам к зачету.

9. Материально-техническое обеспечение дисциплины

Перечень лекционных аудиторий с современными средствами демонстрации – 5-301, 5-314.

Перечень лабораторий современного, высокотехнологичного оборудования, обеспечивающего реализацию ОПОП ВО с учетом направленности подготовки:

- 5-220 – лаборатория защиты информации;

Вычислительное и телекоммуникационное оборудование, необходимое для реализации ОПОП ВО и обеспечения физического доступа к информационным сетям, используемым в образовательном процессе и научно-исследовательской деятельности:

Компьютеры с процессором не хуже Intel i5, ОЗУ – не менее 2 Гб, винчестер 500.Гб, сетевой картой со скоростью передачи данных 1 Гб/сек

Программное обеспечение, необходимое для реализации ОПОП ВО:

- программный комплекс – операционная система Microsoft Windows (№ договора ЭА-269/0503-16 от 20.12.2016, 1800 компьютеров, на которые распространяется право пользования);
- программный комплекс – Microsoft Office (№ договора ЭА-269/0503-16, 1800 компьютеров, на которые распространяется право пользования);
- программный комплекс –Microsoft Visio Pro (№ договора ЭА-269/0503-16, 50 компьютеров, на которые распространяется право пользования);
- Kaspersky Endpoint Security для бизнеса (лицензии 1055/0503-16, 500 users);
- DLP система Falcongaze (лицензионный договор 05/17/2016-1 от 17.05.2016 с ООО «Фалконгейз» , 20 лицензий сроком на 3 года)
- DLP система «Контур информационной безопасности» (лицензионный договор с ООО «Новые поисковые технологии», 20 лицензий сроком 3 года)
- WAF Positive Technologies Application Firewall Education (лицензионный договор с ЗАО Позитив Технолоджис 72-16/EAF от 21.06.2016 сроком на 2 года)
- Операционная система Astra Linux Special Edition (лицензионный договор РБТ-14/1318 -01-ВУЗ от 29.03.2016 , 20 лицензий, нет ограничений срока лицензий)
- Веб-сервер Apache (freeware)
- Microsoft System Center (пробная версия)
- QRadar (пробная версия)

10. Адаптация рабочей программы для лиц с ОВЗ

При обучении инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, обеспечивается возможность беспрепятственного доступа в учебные помещения и пункты питания и другие, необходимые для жизнедеятельности помещения, оборудованные пандусами, лифтами и иными средствами, облегчающими процесс передвижения. Для лиц с ограниченными возможностями здоровья по зрению предусматривается возможность доступа к зданию с собакой-поводырем.

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.